# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/504,005 | 02/14/2000 | Sami Boutros | CISCO-1935 | 7397 |

7590 05/05/2006

JONATHAN VELASCO
SIERRA PATENT GROUP, LTD
P.O. BOX 6149
STATELINE, NV 89449

| EXAMINER | |
|---|---|
| KLIMACH, PAULA W | |
| ART UNIT | PAPER NUMBER |
| 2135 | |

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/504,005 | BOUTROS ET AL. | |
| | Examiner | Art Unit | |
| | Paula W. Klimach | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *02/06/06*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) 27-47 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 27-47 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

This office action is in response to amendment filed on 02/06/06. The amendment filed on 02/06/06 have been entered and made of record. Therefore, presently pending claims are 24-47.

### *Response to Arguments*

Applicant's arguments filed 02/06/06 have been fully considered. The reference of Firth is added to overcome the deficiencies of Williams and O'brien.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claims 27-42 and 46-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over Williams (U.S. Patent 5,996,077) in view of O'Brien et al. (6,658,571 B1), and Firth et al (5,987,517).

*In reference to claim 27,* Williams discloses a hierarchical arrangement of security devices for securing a protected network through a plurality of security devices (abstract). The device consists of a legacy firewall (security device A, principle device) connected to each of a plurality of communication interfaces (public and protected network) and executing at least on inspection module is software code configured to carry out an operation of providing protocol

information for a particular protocol to said firewall core (column 5 line 53 to column 6 line 6); and a new inspection module inserted into an operating memory of said firewall core wherein said new inspection module is software code configured to carry out an operation of providing protocol information for a particular protocol to said firewall core (column 4 lines 1-28 in combination with Fig. 2).

Although Williams discloses the next generation of firewall coexisting with the legacy firewall, Williams does not expressly disclose the new inspection module inserted during operation of said firewall core.

However, O'Brien disclose the separate subsystem consisting of at least one inspection module coupled for communication to the user space, said inspection module configured to provide protocol inspection of data (column 3 lines 39-56), said inspection module is further configured to be installed during the operation of the system (column 3 lines 56-64).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use security modules as in O'Brien to provide protocol inspection in the system of Williams. One of ordinary skill in the art would have been motivated to do this because security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

Williams discloses a firewall core, however Williams does not discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module.

Firth discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module (column 4 lines 13-15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to functionally for a new protocol as in Firth in the system of Williams. One of ordinary skill in the art would have been motivated to do this because it would allow the easy establishment of communications with a variety of computer networks.

*In reference to claim 32*, Williams discloses a hierarchical arrangement of security devices for securing a protected network through a plurality of security devices (abstract). A communication unit wherein said communication unit is operatively coupled to each one of communication interfaces connected to said network (parts 101 and 102 Fig. 2). A firewall core (principle device) and one of said at least one inspection modules (security devices) and wherein each said at least one inspection module is software code configured to carry out the operation of providing protocol information and to inspect data packets of a particular protocol (column 4 lines 1-28 in combination with Fig. 2).

Although Williams discloses the communication to the security devices (Fig 2.) Williams does not disclose a set of call back functions, retrieved from said inspection module, each function providing communication between the firewall core and the inspection module. In addition the firewall core (principle device) disclosed by Williams is not further configured to monitor memory to determine when a new inspection module is loaded into said memory.

O'Brien discloses a set of callback functions, retrieved from said inspection module, each said function providing communication between the security master and said inspection module

(column 5 lines 15-27). In addition the system of O'Brien is configured to monitor a memory to determine when a new inspection module is loaded into said memory (column 5 lines 28-46).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Williams. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

Williams discloses a firewall core, however Williams does not discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module.

Firth discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module (column 4 lines 13-15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to functionally for a new protocol as in Firth in the system of Williams. One of ordinary skill in the art would have been motivated to do this because it would allow the easy establishment of communications with a variety of computer networks.

*In reference to claim 36,* Williams discloses a hierarchical arrangement of security devices for securing a protected network through a plurality of security devices (abstract). The

inspection unit is configured to inspect and authorize data packets (column 4 lines 62-65); a function table which corresponds to a connection table (column 7 lines 31-36).

Although Williams discloses the communication to the security devices (Fig 2.) and a connection table, Williams does not disclose a set of call back functions, retrieved from said inspection module, each function providing communication between the firewall core and the inspection module. In addition the firewall core (principle device) disclosed by Williams is not further configured to monitor memory to determine when a new inspection module is loaded into said memory.

O'Brien discloses a set of callback functions, retrieved from said inspection module, each said function providing communication between the security master and said inspection module (column 5 lines 15-27). In addition the system of O'Brien is configured to monitor a memory to determine when a new inspection module is loaded into said memory (column 5 lines 28-46).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Williams. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

Williams discloses a firewall core, however Williams does not discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the

at least one inspection module.

Firth discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module (column 4 lines 13-15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to functionally for a new protocol as in Firth in the system of Williams. One of ordinary skill in the art would have been motivated to do this because it would allow the easy establishment of communications with a variety of computer networks.

*In reference to claims 39 and 43*, Williams discloses a hierarchical arrangement of security devices for securing a protected network through a plurality of security devices (abstract). The inspection unit is configured to inspect and authorize data packets (column 4 lines 62-65).

O'Brien discloses a) loading an inspection module comprising new protocol inspection knowledge and a function table having a set of callback functions (column 5 lines 1-27); to b) notifying the security master of said inspection module (column 5 lines 12-27); and c) communicating said set of callback functions to the security master (column 5 lines 27-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Williams. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally

executed without additional hardware, or modification to the individual software applications or the underlying operating system.

Williams discloses a firewall core, however Williams does not discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module.

Firth discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module (column 4 lines 13-15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to functionally for a new protocol as in Firth in the system of Williams. One of ordinary skill in the art would have been motivated to do this because it would allow the easy establishment of communications with a variety of computer networks.

*In reference to claim 28,* wherein the firewall core is configured to monitor said operation memory for said new inspection module.

O'Brien is configured to monitor a memory to determine when a new inspection module is loaded into said memory (column 5 lines 28-46).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Williams. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally

executed without additional hardware, or modification to the individual software applications or the underlying operating system.

*In reference to claims 29 and 46,* wherein said inspection module further comprises callback functions, said functions communicated to said firewall core and providing communication between said firewall core and said inspection module.
Williams does not expressly disclose the use of callback functions which communicate to the firewall core and providing communication between the firewall core and said inspection module.

O'Brien discloses a set of callback functions, retrieved from said inspection module, each said function providing communication between the security master and said inspection module (column 5 lines 15-27)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Williams. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

*In reference to claims 30, 37, 42, 47,* wherein each said at least one inspection module and new inspection module are each further configured to indicate to said firewall core for which protocol for data packets said inspection module is configured to provide inspection (column 7

lines 29-47 in combination with column 6 lines 1-6).

*In reference to claims 31 and 34*, wherein each data packet intercepted by said firewall core further includes session information comprising address and port data (column 5 line 60 to column 6 line 6), the firewall core further configured to map said session information for each said data packet to one of said at least one inspection modules and the new inspection module (column 7 lines 35-47).

*In reference to claim 33*, wherein said communication unit further configured to intercept network data communicated via each of said plurality of communication interfaces (Fig. 2).

*In reference to claims 35, 38, 41, and 45*, wherein said communication unit is further configured to communicate a packet between said communication interface and one of said at least one inspection modules (Fig. 2).

*In reference to claims 40, and 44*, further comprising enabling said inspection module, prior to communicating said set of callback function to said firewall core. The new information is used to filter packets therefore the new rules, provided by the security device, are in an enabled state similar to the state of the principle device.

**Claims 43-45** are rejected under 35 U.S.C. 103(a) as being unpatentable over Williams (U.S. Patent 5,996,077) in view of O'Brien et al. (6,658,571 B1).

*In reference to claim 43*, Williams discloses a hierarchical arrangement of security devices for securing a protected network through a plurality of security devices (abstract). The inspection unit is configured to inspect and authorize data packets (column 4 lines 62-65).

O'Brien discloses a) loading an inspection module comprising new protocol inspection

knowledge and a function table having a set of callback functions (column 5 lines 1-27); to b) notifying the security master of said inspection module (column 5 lines 12-27); and c) communicating said set of callback functions to the security master (column 5 lines 27-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Williams. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

Williams discloses a firewall core, however Williams does not discloses a system wherein the new particular protocol is different from each of the particular protocol provided by each of the at least one inspection module.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to functionally for a new protocol as in Firth in the system of Williams. One of ordinary skill in the art would have been motivated to do this because it would allow the easy establishment of communications with a variety of computer networks.

*In reference to claim 44*, further comprising enabling said inspection module, prior to communicating said set of callback function to said firewall core. The new information is used to filter packets therefore the new rules, provided by the security device, are in an enabled state similar to the state of the principle device.

*In reference to claim 45,* wherein said communication unit is further configured to communicate a packet between said communication interface and one of said at least one inspection modules (Fig. 2).

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, May 01, 2006

HOSUK SONG
PRIMARY EXAMINER